FortiOS - Release Notes

VERSION 5.6.2

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

January 08, 2018

FortiOS 5.6.2 Release Notes

01-562-444995-20180108

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-08-17	Initial release.
2017-08-29	Removed 440412 from *Known Issues*.
2017-08-30	Added section *Special branch supported models* to *Introduction*.
2017-08-31	Added new section *FortiGate-VM64-Azure upgrade* to *Upgrade Information* > *Upgrading to FortiOS 5.6.2*.
2017-09-06	Added 435283 to *Known Issues*.
2017-10-06	Updated note in *Upgrading to FortiOS 5.6.2*.
2017-10-11	Updated *Known Issues* > *FortiSwitch-Controller/FortiLink* to update 369099 description, and remove 404399 and 415380. Updated *Product Integration and Support* > *SSL VPN support* > *SSL VPN host compatibility* list.
2018-01-08	Added 454259 to *Known Issues*.

Introduction

This document provides the following information for FortiOS 5.6.2 build 1486:

- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 5.6.2 supports the following models.

FortiGate	FG-30D, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30D-POE, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG- 200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240D-POE, FG-280D-POE, FG-300D, FG-400D, FG-500D, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001C, FG-5001D
FortiWiFi	FWF-30D, FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-30D-POE, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM
FortiOS Carrier	FortiOS Carrier 5.6.2 images are delivered upon request and are not available on the customer support firmware download page.

Special branch supported models

The following models are released on a special branch of FortiOS5.6.2. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1486.

FG-VM64-AZURE	is released on build 4005.
FG-VM64-AZUREONDEMAND	is released on build 4005.

What's new in FortiOS 5.6.2

For a list of new features and enhancements that have been made in FortiOS 5.6.2, see the *What's New for FortiOS 5.6.2* document.

Special Notices

Built-in certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

FortiGate and FortiWiFi-92D hardware limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form
- IPv6 packets being dropped
- FortiSwitch devices failing to be discovered
- Spanning tree loops may result depending on the network topology

FG-92D and FWF-92D do not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config global
   set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed
- BPDUs are dropped and therefore no STP loop results
- PPPoE packets are dropped
- IPv6 packets are dropped
- FortiSwitch devices are not discovered
- HA may fail to form depending the network topology

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result

FG-900D and FG-1000D

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip.

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

FortiGate-VM 5.6 for VMware ESXi

Upon upgrading to FortiOS 5.6.2, FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

FortiClient profile changes

With introduction of the Security Fabric, FortiClient profiles will be updated on FortiGate. FortiClient profiles and FortiGate are now primarily used for Endpoint Compliance, and FortiClient Enterprise Management Server (EMS) is now used for FortiClient deployment and provisioning.

The FortiClient profile on FortiGate is for FortiClient features related to compliance, such as Antivirus, Web Filter, Vulnerability Scan, and Application Firewall. You may set the *Non-Compliance Action* setting to *Block* or *Warn*. FortiClient users can change their features locally to meet the FortiGate compliance criteria. You can also use FortiClient EMS to centrally provision endpoints. The EMS also includes support for additional features, such as VPN tunnels or other advanced options. For more information, see the *FortiOS Handbook – Security Profiles*.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

DLP, AV

In 5.2, Block page was sent to client with HTTP status code `200` by default. In 5.4 and later, Block page is sent to client with a clearer HTTP status code of `403 Forbidden`.

Upgrade Information

Upgrading to FortiOS 5.6.2

FortiOS version 5.6.2 officially supports upgrading from version 5.4.4, 5.4.5, 5.6.0, and 5.6.1. To upgrade from other versions, see Supported Upgrade Paths.

If you are upgrading from version 5.6.1, this caution does not apply.

Before upgrading, ensure that port 4433 is not used for `admin-port` or `admin-sport` (in `config system global`), or for SSL VPN (in `config vpn ssl settings`).

If you are using port 4433, you must change `admin-port`, `admin-sport`, or the SSL VPN port to another port number before upgrading.

FortiGate-VM64-Azure upgrade

You can upgrade from the GUI or CLI. Because some configurations are not kept in the upgrade, we recommend you do a factory reset using `execute factoryreset`, and then reconfigure the VM.

Your original VM license is kept in the upgrade.

Security Fabric upgrade

FortiOS 5.6.2 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 5.6.0
- FortiClient 5.6.0
- FortiClient EMS 1.2.1
- FortiAP 5.4.2 and later
- FortiSwitch 3.5.2 and later

Upgrade the firmware of each product in the correct order. This maintains network connectivity without the need to use manual steps.

Before upgrading any product, you must read the *FortiOS Security Fabric Upgrade Guide*.

FortiClient profiles

After upgrading from FortiOS 5.4.0 to 5.4.1 and later, your FortiClient profiles will be changed to remove a number of options that are no longer supported. After upgrading, review your FortiClient profiles to make sure they are configured appropriately for your requirements and either modify them if required or create new ones.

The following FortiClient Profile features are no longer supported by FortiOS 5.4.1 and later:

- Advanced FortiClient profiles (XML configuration)
- Advanced configuration, such as configuring CA certificates, unregister option, FortiManager updates, dashboard Banner, client-based logging when on-net, and Single Sign-on Mobility Agent
- VPN provisioning
- Advanced AntiVirus settings, such as Scheduled Scan, Scan with FortiSandbox, and Excluded Paths
- Client-side web filtering when on-net
- iOS and Android configuration by using the FortiOS GUI

With FortiOS 5.6.2, endpoints in the Security Fabric require FortiClient 5.6.0. You can use FortiClient 5.4.3 for VPN (IPsec VPN, or SSL VPN) connections to FortiOS 5.6.2, but not for Security Fabric functions.

It is recommended that you use FortiClient Enterprise Management Server (EMS) for detailed Endpoint deployment and provisioning.

FortiGate-VM 5.6 for VMware ESXi

Upon upgrading to FortiOS 5.6.2, FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

If you have long VDOM names, you must shorten the long VDOM names (maximum 11 characters) before downgrading:

1. Back up your configuration.
2. In the backup configuration, replace all long VDOM names with its corresponding short VDOM name. For example, replace `edit <long_vdom_name>/<short_name>` with `edit <short_name>/<short_name>`.
3. Restore the configuration.
4. Perform the downgrade.

Amazon AWS enhanced networking compatibility issue

With this new enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 5.6.2 image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 5.6.2 to older versions, running the enhanced nic driver is not allowed. The following AWS instances are affected:

- C3
- C4
- R3
- I2
- M4
- D2

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiOS 5.6.2 support

The following table lists 5.6.2 product integration and support information:

Web Browsers	• Microsoft Edge 38 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 54 • Google Chrome version 59 • Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 40 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 53 • Google Chrome version 58 • Apple Safari version 10 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Security Fabric upgrade on page 11. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Security Fabric upgrade on page 11. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	See important compatibility information in Security Fabric upgrade on page 11. • 5.6.0 If FortiClient is being managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate.

FortiClient iOS	• 5.4.3 and later
FortiClient Android and FortiClient VPN Android	• 5.4.1 and later
FortiAP	• 5.4.2 and later • 5.6.0
FortiAP-S	• 5.4.3 and later • 5.6.0
FortiSwitch OS (FortiLink support)	• 3.5.6 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later

Fortinet Single Sign-On (FSSO)	• 5.0 build 0254 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.

FortiExtender	• 3.1.1 and later
AV Engine	• 5.247
IPS Engine	• 3.426
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, and 2012 R2

Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish (Spain)	✔

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04	2333. Download from the Fortinet Developer Network https://fndn.fortinet.net.

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit) Microsoft Windows 8 / 8.1 (32-bit & 64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 54 Google Chrome version 59
Microsoft Windows 10 (64-bit)	Microsoft Edge Microsoft Internet Explorer version 11 Mozilla Firefox version 54 Google Chrome version 59
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54

Operating System	Web Browser
Mac OS 10.11.1	Apple Safari version 9 Mozilla Firefox version 54 Google Chrome version 59
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

It is recommended to verify the accuracy of the GUID for the software you are using for SSL VPN host check. The following Knowledge Base article at http://kb.fortinet.com/ describes how to identify the GUID for antivirus and firewall products: How to add non listed 3rd Party AntiVirus and Firewall product to the FortiGate SSL VPN Host check.

After verifying GUIDs, you can update GUIDs in FortiOS by using the `config vpn ssl web host-check-software` command.

Following is an example of how to update the GUID for AVG Internet Security 2017 on Windows 7 and Windows 10 by using the FortiOS CLI.

The GUIDs in this example are only for AVG Internet Security 2017 on Windows 7 and Windows 10. The GUIDs might be different for other versions of the software and other operation systems.

To update GUIDs in FortiOS:

1. Use the `config vpn ssl web host-check-software` command to edit the `AVG-Internet-Security-AV` variable to set the following GUID for AVG Internet Security 2017: `4D41356F-32AD-7C42-C820-63775EE4F413`.
2. Edit the `AVG-Internet-Security-FW` variable to set the following GUID: `757AB44A-78C2-7D1A-E37F-CA42A037B368`.

Resolved Issues

The following issues have been fixed in version 5.6.2. For inquires about a particular bug, please contact Customer Service & Support.

GUI

Bug ID	Description
442145	httpsd daemon signal 11 crash due to missing default parameter for `/endpoint-control/avatar/download`.
442939	Switch-controller `Managed FortiSwitch` failed to be displayed and triggered `Internal Server Error`.

SSL VPN

Bug ID	Description
442808	SSL VPN daemon crash and users disconnected when any one of tunnel users log out.

Known Issues

The following issues have been identified in version 5.6.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Application Control

Bug ID	Description
435951	Traffic keeps going through the `DENY` NGFW policy configured with URL category.
441996	No UTM AppCtrl log for signature `Gmail_Attachment.Download` when action is blocked.

DLP

Bug ID	Description
435283	`block-page-status-code` doesn't work for HTTP status code of the DLP replacement message.

Firewall

Bug ID	Description
434959	NGFW policy with App Control policy blocks traffic.

FortiGate 3815D

Bug ID	Description
385860	FG-3815D does not support 1GE SFP transceivers.

FortiLink

Bug ID	Description
434470	Explicit policy for traffic originating from interface dedicated to FortiLink.
441300	Limited options in FortiLink quarantine stanza to use, giving users no way to trigger the quarantine function.

FortiSwitch-Controller/FortiLink

Bug ID	Description
304199	Using HA with FortiLink can encounter traffic loss during failover.
357360	DHCP snooping may not work on IPv6.
369099	FortiSwitch-Controller configurations are not automatically migrated when upgrading from 5.4.0.
408082	Operating a dedicated hardware switch into FortiLink changes STP from *enable* to *disable*.
445373	For 802.1X, FortiSwitch port disappeared after upgrading FortiGate from 5.6.0 to 5.6.1 with 802.1X enabled without security-group/user-group.

FortiView

Bug ID	Description
366627	FortiView Cloud Application may display the incorrect drill down *File and Session* list in the *Applications View*.
368644	*Physical Topology: Physical Connection* of stacked FortiSwitch may be incorrect.
375172	FortiGate under a FortiSwitch may be shown directly connected to an upstream FortiGate.
402507	In physical/logical topology, threat drill down fails and keeps GUI loading unexpectedly.
408100	Log fields are not aligned with columns after drill down on FortiView and Log details.
441835	Drill down a auth-failed wifi client entry in "Failed Authentication" could not display detail logs when CSF enabled.
442238	FortiView VPN map can’t display Google map (199 dialup VPN tunnel).
442367	In *FortiView* > *Cloud Applications*, when the cloud users column is empty, drill down will not load.

GUI

Bug ID	Description
374247	GUI list may list another VDOM interface when editing a redundant interface.
375036	The *Archived Data* in the *Sniffer Traffic* log may not display detailed content and download.

Bug ID	Description
375383	If the policy includes the *wan-load-balance* interface, the policy list page may receive a javascript error when clicking the search box.
398397	Slowness in accessing *Policy* and *Address* page in GUI after upgrading from 5.2.2 to 5.4.1.
402775	Add multiple ports and port range support in the explicit FTP/web proxy.
403146	Slow GUI *Policy* tab with more than 600 policies.
412401	Incorrect throughput reading in *GUI-System-HA* page.
439185	AV quarantine cannot be viewed and downloaded from detail panel when source is FortiAnalyzer.
442231	Link cannot show different colors based on link usage legend in logical topology real time view.
454259	The *Policy* list page does not display tooltips for policy comments.

HA

Bug ID	Description
439152	FGSP - standalone config sync - synchronizes BGP neighbor.
441078	The time duration of packet-transporting process stops to pre-master node after HA failover takes too long.
441716	Traffic stops when `load-balance-all` is enabled in active-active HA when `npu_vlink` is used in the path.
436585	Issues with different hardware generation when operating in a HA cluster.

IPsec

Bug ID	Description
416102	Traffic over IPsec VPN gets dropped after two pings when it is getting offloaded to NPU.

Log & Report

Bug ID	Description
412649	In NGFW Policy mode, FGT does not create webfilter logs.
438858	Synchronized log destination with *Log View* and *FortiView* display source.

Bug ID	Description
441476	Rolled log file is not uploaded to FTP server by `max-log-file-size`.

Proxy

Bug ID	Description
442252	WAD stops forwarding traffic on both transparent proxy and explicit web proxy after IPS test over web proxy.

Security Fabric

Bug ID	Description
403229	In FortiView display from FortiAnalyzer, the upstream FortiGate cannot drill down to final level for downstream traffic.
409156	In Security Fabric Audit, The unlicensed FDS FortiGate shouldn't be marked *Passed* in *Firmware & Subscriptions*.
411368	In FortiView with FortiAnalyzer, the combined MAC address is displayed in the *Device* field.
414013	Log Settings shows `Internal CLI error` when enabling historical FortiView at the same time as disk logging.

SSL VPN

Bug ID	Description
405239	URL rewritten incorrectly for a specific page in application server.

System

Bug ID	Description
290708	`nturbo` may not support CAPWAP traffic.
295292	If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
304199	FortiLink traffic is lost in HA mode.
364280	User cannot use `ssh-dss` algorithm to login to FortiGate via SSH.
436580	`PDQ_ISW_SSE` drops at +/-100K CPS on FG-3700D with FOS 5.4 only.

Bug ID	Description
436746	NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.
437801	FG-30E WAN interface MTU override drop packet issue.
438405	HRX/PKTCHK drops over NP6 with 1.5 Gbps.
439126	Auto-script using diagnose command fails with `Unknown action 0` after rebooting FortiGate.
439553	Virtual wire pair config missing after reboot.
440411	Monitor NP6 IPsec engine status.
440448	FG-800C will not get IP on the LTE-modem interface using Novatel U620.
441532	Suggest to add SNMP/CLI monitoring capabilities of NP6 session table.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.